

JP2002-232962A

MOBILE COMMUNICATION AUTHENTICATION INTERWORKING SYSTEM

Date of publication of application : 16.08.2002

Application number : 2001-030543

Applicant : KDDI CORP

Date of filing : 07.02.2001

Inventor : OHASHI MASAYOSHI

TANAKA TOSHIKI

NEMOTO TAKASHI

Abstract:

PROBLEM TO BE SOLVED: To provide a mobile communication authentication interworking system that can efficiently execute CR(Challenge Response) authentication with high security in roaming between systems where a random number transmission bit length differs between networks without revising an existing protocol.

SOLUTION: The interworking system utilizes a configuration that for example, in the case of roaming from an ANSI(American National Standards Institute)-41 system to a GSM(Global System for Mobile Communications), the CR set generated by the home ANSI-41 system is basically included as it is by the GSM system (excess bits are filled by zero or the like) and transmitted to attain communication of a random number and an arithmetic result with a terminal roaming to the GSM system.

| (51) Int.Cl. ⁷ | 識別記号 | F I | テマコード* (参考) |
|---------------------------|------|--------------|-------------------|
| H 0 4 Q 7/38 | | H 0 4 B 7/26 | 1 0 9 R 5 J 1 0 4 |
| H 0 4 L 9/32 | | | 1 0 9 G 5 K 0 6 7 |
| H 0 4 Q 7/34 | | H 0 4 L 9/00 | 6 7 5 C |
| | | H 0 4 Q 7/04 | C |

審査請求 未請求 請求項の数 1 O L (全 7 頁)

(21) 出願番号 特願2001-30543(P2001-30543)

(22) 出願日 平成13年2月7日 (2001.2.7)

(71) 出願人 000208891

ケイディーディーアイ株式会社

東京都新宿区西新宿二丁目3番2号

(72) 発明者 大橋 正良

埼玉県上福岡市大原2-1-15 株式会社

ケイディディ研究所内

(72) 発明者 田中 俊昭

埼玉県上福岡市大原2-1-15 株式会社

ケイディディ研究所内

(74) 代理人 100069257

弁理士 大塚 学

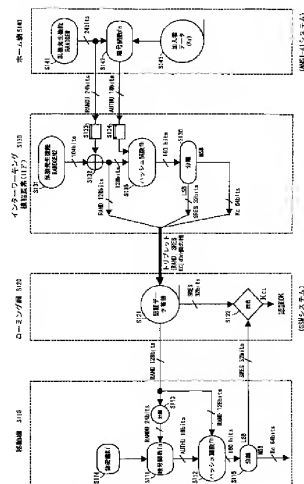
最終頁に続く

(54) 【発明の名称】 移動通信認証インターワーキング方式

(57) 【要約】

【課題】既存のプロトコルに変更をきたすことなく、乱数伝達ビット長が網間で異なるシステム間のローミングにおけるCR認証の効率的でかつセキュリティ上安全な実行を可能とする移動通信認証インターワーキング方式を提供する。

【解決手段】例えば、ANSI-41からGSMへのローミングの場合に、ホームのANSI-41システムが生成したCR組は、基本的にはそのままGSMシステムに包みこんで（余分なビット分は0等により埋めて）伝送することで乱数、演算結果をGSMシステムにローミングしている端末とやりとりすることが可能であることを利用する構成を有している。



【特許請求の範囲】

【請求項1】 あらかじめ同一の秘密鍵が移動機と該移動機の本来属する移動通信網であるホーム網のデータベース内に設定、記憶されるとともに、該秘密鍵と同一の暗号関数が前記移動機と前記ホーム網に備わっており、該移動機が前記秘密鍵を有していることを、網側から該移動機に乱数を用いて送出し、該移動機ではその乱数と該移動機の前記秘密鍵を前記暗号関数の入力として演算を行った結果を前記移動通信網に送付することで証明することにより、該移動機の正当性を確認するチャレンジ・レスポンス認証方式が実装された移動通信網が存在する系において、

該移動機の移動先の移動通信網であるローミング先網における乱数伝達ビット長が、前記ホーム網で用いられる乱数伝達ビット長よりも長い場合に、両網間をまたがってインターワークを行うインターワーキング機能要素において、乱数発生機能と、安全な方向性の特徴を有するハッシュ関数を配備し、

前記ホーム網より前記インターワーキング機能要素に送出されたチャレンジ・レスポンスの1組に対して、該インターワーキング機能要素において、適切な個数の乱数 n 個を発生させ、この乱数とチャレンジを結合させた結果を新たなチャレンジにすると共に、新たなチャレンジならびにレスポンスを前記ハッシュ関数に通すことにより新たなレスポンスを生成し、この過程を n 回繰り返すことにより、 n 組のチャレンジ・レスポンスを発生させて、前記ローミング先網に転送して、該ローミング先網において n 回の認証を可能にすることを特徴とする移動通信認証インターワーキング方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、方式が異なっている携帯電話等の複数の移動通信網において、方式の異なる移動網に移動機がアクセス（ローミング）して通信を行おうとする場合、その移動機が当該移動機の本来属するホームの移動網の正当な移動機であることをローミング先の移動網が確認するための、移動通信網の通信制御方式に関する。

【0002】

【従来の技術】移動通信網を介する通信では、固定系の通信形態とは異なり、無線通信周波を介して相手移動機と接続されるため、接続される移動機が確かに所望の移動機であるかどうかを網側からは必ずしも明確に判明しない。そのため何らかの手法を用いて、網は接続移動機の正当性を確認する必要がある。この正当性確認は認証と呼ばれている。認証に当たっては、無線通信周波が傍受されやすい性質を持っているため、仮に盗聴を受けたとしても、移動機は、後に盗聴者が不正な移動機を用い、正当な移動機の振りをして移動網にアクセスされない工夫が必要になる。

【0003】このため現在のデジタル移動通信網では、秘密鍵暗号方式に基づくチャレンジ・レスポンス認証（以下CR認証と呼ぶ）が幅広く用いられている。以下図2を用いて同方式を説明する。CR認証方式では、移動通信網と移動機は共通の秘密鍵暗号関数 f を所持する。その秘密鍵暗号関数 f は2つの変数を持ち、一つは秘密鍵 K_i 、一つは乱数 $RAND$ である。秘密鍵 K_i はパラメータとなるので、この関数出力を $f(K_i, RAND)$ と記し、その結果の値を $SRES$ と呼ぶ。

【0004】移動網は、自網に所属するすべての正当な移動機の秘密鍵（ K_i ）を有する（S1）。秘密鍵（ K_i ）としては、移動機すべてに異なった値が割り当てられる。正当な移動機は、それぞれ自らの秘密鍵 K_i を、外部からの読み出しの攻撃に対し、たとえばICカードに格納するなど、物理的に安全に保持している（S2）。

【0005】CR認証に際して、移動機はまず自らの移動機番号を移動網に伝える（S3）。移動網はデータベース検索によって、対象移動機の秘密鍵 K_i を得る。移動網は、乱数（チャレンジ） $RAND$ を発生し（S4）、移動機に送出する（S5）。移動機は受け取った乱数 $RAND$ と自分の秘密鍵より関数 f を用いて暗号演算を行い（S6）、その演算結果（レスポンス）を $SRES$ として移動網に送り返す（S7）。移動網も K_i 、 f を有するので、同じ演算を行う（S8）。その結果が移動機より送り返されてきた $SRES$ と一致すれば（YES）、認証成功であり、さもなくば失敗（NO）となる。

【0006】CR認証では、移動機が正当な秘密鍵 K_i を有していることを、無線区間上で直接移動網に提示することなく、 $RAND$ と $SRES$ の受け渡しのみで移動網に示すことができるため、盗聴によっても K_i を知られることのない有効な方式である。さらに $RAND$ は移動網によって任意に調べ、その値に応じて移動機が返す正しい $SRES$ の値は異なるため、複数回不正な移動機が傍受を行っても、自らが正当な移動機になりますことはできない。従って、CR認証は、移動通信システムのセキュリティを確保する観点から非常に優れた方式の一つである。以下の説明では、すべてCR認証を用いると仮定する。

【0007】次にローミングについて説明を行う。ローミングとは、移動機が自網以外の網にアクセスして通信を行う機能をいう。このとき移動機が本来属している網をホーム網、現在アクセスしている網をローミング先網と呼ぶ。ローミング時には、ローミング先網は通信に先立ち、アクセスしてきた移動機がホーム網に正当に登録された移動機であるかどうかを認証する必要がある。しかしながら、ローミング先網は、ローミングしてきた移動機の秘密鍵を持たず、また必ずしもホーム網と同一の暗号関数 f を採用しているわけではない。ただし、両網

で共通のCR認証スキームを採用し、チャレンジ、レスポンスいずれも同じ情報長を有している場合には、ホーム網が対象となる移動機の秘密鍵Kiを用いて認証に必要な一つもしくは複数のチャレンジ・レスポンスの組(以下CR組と呼ぶ)〔RAND, SRES〕を生成し、ローミング先網に渡せば、網からチャレンジRANDを移動機に投げかけ、移動機より返された結果がホーム網より受け取ったSRESと合致するか否かを検証することで、ホーム網と同様に認証を行うことができる。これは現在のGSM(Global System for Mobile Communications)システムにおいて広く用いられている方式である。

【0008】

【発明が解決しようとする課題】上記のようにローミング時にCR組を渡す方式は、各網の暗号関数fの一致を必要としない優れた方式である。しかしながら、例えば北米標準であるANSI-41のようなシステムにおいては、一度にホーム網よりローミング先ネットワークに渡せるCR組が1組(これはユニークチャレンジと呼ばれる)であるのに対し、例えば欧州標準であるGSMシステムでは、複数組を一度に渡すことが可能になっている。GSMシステムにて複数のチャレンジ・レスポンスを渡すためにインターワーキング機能要素を介し、ANSI-41システムにて複数のメッセージを受受するのはプロトコルの面からは非常に非効率である。

【0009】本発明は、既存のプロトコルに変更をきたすことなく、このような乱数伝達ビット長が網間で異なるシステム間のローミングにおけるCR認証の効率の得かつセキュリティ上安全な実行を可能とする移動通信認証インターワーキング方式を提供することを目的としている。

【0010】

【課題を解決するための手段】本発明によれば上述の問題点は前記特許請求の範囲に記載した手段により解決される。すなわち、本発明は、あらかじめ同一の秘密鍵が移動機と該移動機の本来属する移動通信網であるホーム網のデータベース内に設定、記憶されるとともに、該秘密鍵と同一の暗号関数が前記移動機と前記ホーム網に備わっており、該移動機が前記秘密鍵を有していることを、網側から該移動機に乱数を用いて送出し、該移動機ではその乱数と該移動機の前記秘密鍵を前記暗号関数の入力として演算を行った結果を前記移動通信網に返すことで証明することにより、該移動機の正当性を確認するチャレンジ・レスポンス認証方式が実装された移動通信網が存在する系において、該移動機の移動先の移動通信網であるローミング先網における乱数伝達ビット長が、前記ホーム網で用いられる乱数伝達ビット長よりも長い場合に、両網間をまたがってインターワークを行うインターワーキング機能要素において、乱数発生機能と、安全な一方方向性の特徴を有するハッシュ関数を配備し、前

記ホーム網より前記インターワーキング機能要素に送出されたチャレンジ・レスポンスの1組に対して、該インターワーキング機能要素において、適切な個数の乱数n個を発生させ、この乱数とチャレンジを結合させた結果を新たなチャレンジにすると共に、新たなチャレンジならびにレスポンスを前記ハッシュ関数に通すことにより新たなレスポンスを生成し、この過程をn回繰り返すことにより、n組のチャレンジ・レスポンスを発生させて、前記ローミング先網に転送して、該ローミング先網においてn回の認証を可能にすることを特徴とする構成を有している。

【0011】【発明の原理】ANSI-41システムにて使用される乱数、演算結果はそれぞれ、24ビット、18ビットである。またGSMシステムにて使用される乱数、演算結果は128ビット、32ビットである。本発明は、例えば、ANSI-41からGSMへのローミングの場合に着目すると、ホームのANSI-41システムが生成したCR組は、基本的にはそのままGSMシステムに包みこんで(余分なビット分は0等により埋めて)伝送することで乱数、演算結果をGSMシステムにローミングしている端末とやりとりすることが可能であることを利用するものである。

【0012】

【発明の実施の形態】以下本発明の作用等に関し、実施例に基づいてさらに詳細に説明する。

【0013】【実施例1】図1は、ANSI-41からGSMシステムにローミングを行う際の実施例を示している。本例では、ホーム網S140および移動機S110は暗号関数f(a(S142ならびにS111))を有するものとし、その共通の秘密鍵をKiとする。Kiはホーム網においては、安全な加入者データベースS143に、移動機においては安全なメモリS114に格納されているものとする。ホーム網における乱数RANDのビット長は24ビット、演算結果AUTHUのビット長は18ビットとする。

【0014】一方、ローミング先網(S120)のGSMでの乱数RANDのビット長は128ビット、演算結果SRESビット長は32ビットとする。インターワーキングを司る機能要素IIF(Interworking and Interoperability Function)S130および移動機S110は、セキュリティ上安全な一方方向性の性質を有するハッシュ関数fh(S135およびS112)を有するものとし、任意の長さのビット列より、ある長さの安全なハッシュ結果を生成できるものとする。ここではハッシュ関数を例えばSHA-1とし、その出力を160ビットとする。加えて移動機S110とインターワーキング機能要素(IIF)S130において暗号化のための鍵Kcは64ビット長とする。

【0015】移動機がローミング先GSM網S120においてローミング要求を発すると、ローミング先GSM

網S120は移動機番号を得てホーム網S140に通知する。ANSI-41ホーム網S140はそのデータベースS143中より対応する移動機の秘密鍵Kiを取り出す。実際のANSI-41システムでは、Kiに相当するものは真の鍵に各種識別子を付加した値になるが、ここではこれらを含めてKiと記す。次いでANSI-41ホーム網S140は、ユニークチャレンジと呼ばれる一組の乱数RANDUならびに演算結果

【数1】

$$AUTHU = fa \cdot Ki \cdot (RANDU) \quad \cdots (1)$$

$$RANDi = RANDi \parallel RANDU \quad \cdots (2)$$

$$SRESi = \text{LSB32bits of } \{fh(RANDU, AUTHU)\} = \text{LSB32ts of } \{fh(RANDi \parallel RANDU, fa \cdot Ki(RANDU))\} \quad \cdots (3)$$

$$Kci = \text{MSB64bit of } \{fh(RANDi, AUTHU)\} = \text{MSB64bit of } \{fh(RANDi \parallel RANDU, fa \cdot Ki(RANDU))\} \quad (i=1, \dots, n) \quad \cdots (4)$$

(\parallel は結合を表し、図1ではS132に対応するトリプレット $[RANDi, SRESi, Kci]$ ($i=1, \dots, n$) のn個の組)

をインターワーキング機能要素(IIF)S130にて生成する。(IIF)S130はこれらをローミング先GSM網S120に送付する。

【0017】ローミング網S120ではこれらのトリプレットをデータベースS121に格納しておき、認証が必要になる度にこれらのトリプレットを1組ずつ取り出し、 $RANDi$ を移動機S110に対して送付する。移動機S110は、受信した128ビットの $RANDi$ を(IIF)S130での結合規則S132に則り、S113にて24ビットの $RANDU$ を抽出する。

【0018】移動機S110にはKiがS114に格納されているため、式(1)に従い $AUTHU$ を計算した後、式(3)、(4)に従い、 $SRESi$ 、 Kci を作成し、 $SRESi$ をローミング網S120に返す。ローミング網S120には(IIF)S120より送付されてきた $SRESi$ があるので、S122にて移動機S110から送付された値と照合を行い、値が一致すれば認証成功であり、一致しなければ失敗となる。認証成功の際には、 Kci がこの後暗号通信を行うためのセッション鍵を与える。トリプレットは使い捨てである。認証がn回行われると、ローミング網S120中のトリプレットを使い尽くすため、新規にインターワーキング機能要素(IIF)S130にトリプレット送付要求を送る。

(IIF)S130は再びANSI-41ホーム網S140に対して初期登録と同じ要求を行い、ユニークチャレンジ情報を得てn組のトリプレットを作成し、以下同様の処理を継続する。

【0019】なお、本発明例では移動機を1なる機能要素として取り扱ったが、例えばGSMシステムでは、認証演算は移動機に装着されるSIM (Subscriber Identity Module) と呼ばれるICカード中に格納されている。この場合も、SIMが本発明における移動機の機能を果

を発生し、インターワーキング機能要素(IIF)S130に転送する。

【0016】インターワーキング機能要素(IIF)S130では、これらの値をレジスタS133、S134に保持しておく。次にS130に配置された乱数発生器S131により、GSM網が要求する組数nだけの104ビットの乱数(RND1, RND2, ..., RNDn)を発生させ、

【数2】

たすことにより、本発明が実施可能である。

【0020】インターワーキング機能要素(IIF)S130ならびに移動機S110にはハッシュ関数fhが用いられているが、もしこの関数fhを公知にしておきたくない場合には、あらかじめシステムに決められた秘密鍵Khを用意しておき、(IIF)S130ならびに移動機S110内にこの値を格納し、式(3)、(4)の処理にて、 $fh(RANDi, AUTHU)$ を、 $fh(RANDi, AUTHU, Kh)$ とすればよい。

【0021】

【発明の効果】以上述べたように、本発明による移動通信認証方式を用いることにより、インターワーキング機能要素において一個のANSI-41用のCR組から、安全に複数のGSMシステム用CR組を生成することができ、ANSI-41/GSMのいずれのシステムにも変更を来すことなく、ANSI-41からGSMへの認証インターワーキングが可能となる。

【0022】また安全性の面からは、新たに生成されたn個のトリプレットから、ホーム網の加入者に関する秘密情報を探り出すことは極めて困難である。すなわち、n個のトリプレットに含まれる $SRESi$ 、 Kci は、安全な一方方向性ハッシュ関数の出力であるため、仮に無線区間に盗聴者がいるものとして、観測される $RANDi$ 、 $SRESi$ より入力値 $AUTHU$ を探り出すのは大変困難である。たとえこれが割り出されたとしても、そこで利用するのは($RANDU$, $AUTHU$)という、通常のANSI-41におけるユニークチャレンジ相当の情報である。従ってこの状況においてさえ、通常のANSI-41と同等のセキュリティが確保されているといえる。

【0023】なお例1においては対象をANSI-41システムからGSMシステムへのローミングとして説明を加えたが、基本的にチャレンジ・レスポンスをベースとするシステム間の認証インターワークで、かつローミング先システムの乱数伝達長がホーム網における乱数伝

達長に比べて長い場合には、本発明が適用可能である。

【図面の簡単な説明】

【図１】本発明の構成及び動作を説明するための動作フローを含むブロック図である。

【図２】本発明に用いるチャレンジ・レスポンス認証方式を説明するためのフロー図である。

【符号の説明】

S 1 1 0 移動機

S 1 1 1 暗号関数 f a

S 1 1 2 ハッシュ関数 f h

S 1 1 3 分離回路

S 1 1 4 秘密鍵 K_i

S 1 1 5 分離回路

S 1 2 0 ローミング網（GSMシステム）

S 1 2 1 認証データ蓄積

S 1 2 2 照合回路

S 1 3 0 インターワーキング機能要素（I I F）

S 1 3 1 乱数発生機能（RANDGENZ）

S 1 3 2 結合規則

S 1 3 3, S 1 3 4 レジスタ

S 1 3 5 ハッシュ関数 f h

S 1 3 6 分離器

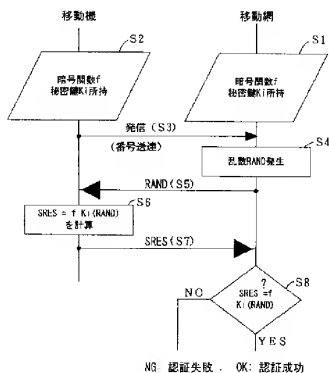
S 1 4 0 ホーム網（ANSI-41）

S 1 4 1 乱数発生機能（RANDGEN）

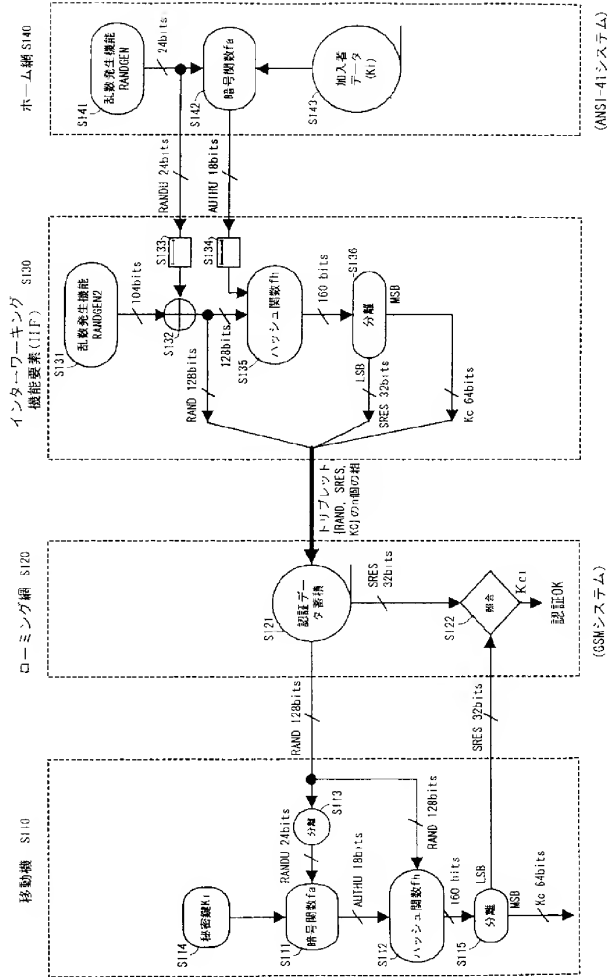
S 1 4 2 暗号関数 f a

S 1 4 3 加入者データ（ K_i ）

【図２】



【図 1】



フロントページの続き

(72)発明者 根本 隆史

埼玉県上福岡市大原 2-1-15 株式会社

ケイディディ研究所内

F ターム(参考) 5J104 AA04 AA07 KA02 KA04 KA06

KA08 KA21 NA03 NA11 NA12

NA22 PA02

5K067 AA33 BB04 DD17 EE04 EE10

HH11 HH17 HH21 HH23